Brian Sandoval
Governor

Nevada Department of Public Safety

James M. Wright
Director

General Services Division
333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6262 – Fax (775) 687-3289
www.gsd.nv.gov

Julie Butler
Division Administrator

Physical and Technical Security Requirements For Nevada Livescan Installations

The following are hardware and service requirements that are required for establishing a connection to the Nevada Department of Public Safety for the purposes of submitting fingerprints electronically.

For Agencies That Connect Directly To Nevada ONLY

- **Agencies connected to or through SilverNet** (state government and criminal justice agencies only) should supply their EITS routable address (10.0.0.1 – 10.255.255.254).
- **Agencies using an Internet connection** need to supply a static IP address that is routable on the Internet. Of the IP address range from 0.0.0.0 to 223.255.255.255, the following address ranges are NOT routable on the Internet:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- **A firewall capable of creating an IPSEC VPN tunnel that also meets Federal Information Processing Standards (FIPS) 140-2** for the encryption engine. DPS strongly recommends using the Cisco ASA 5505 or another Cisco Product in the ASA series. Using this product will enhance the ability for "canned" configurations. If you want to see if your device meets the FOPS 140-2 standard, check the list at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. At this site, the products are listed by date of approval and not by manufacturer or model so you may need to hunt around for your specific product. If you find another product, there should be text that says "*Validated to FIPS 140-2*". If you product is not in the list or the entry for your product lacks this endorsement, you may not use that product to connect to Nevada DPS.
  - All livescan equipment to include printers, need to be "inside" or "behind" a firewall that protects them from the rest of the agency network.
  - The firewall must establish a LAN-to-LAN IPSEC VPN tunnel with DPS. The tunnel shall not be shared with any other network traffic. An exception to this requirement is terminals used *exclusively* for JLink access.

- The encryption for the VPN tunnel shall have been demonstrated to meet FIPS 140-2 encryption standards.
- The firewall shall not have any inbound exceptions other than those used for internally managing the livescan, if any.

For Agencies That Connect To A Channeling Service ONLY

- A firewall must separate all Livescan equipment from the general purpose network. The firewall must be located inside the physically secure Location.
- The firewall should not have any inbound exceptions other than those required to manage the Livescan equipment. Exceptions will be as restrictive as possible.
- Configure your Livescan as directed by the channeling service provider.

Physical Security For ALL Livescan Agencies

- The Livescan should be in a physically secure area.
- All entry points to the secure area should be marked with signs or placards that say "Restricted Area – Authorized Personnel Only" or similar language.
- A physically secure area that is accessible only by those who are authorized to use the device, plus those who have passed fingerprint-based background investigations. All others must be continuously escorted while in the Livescan area. This includes custodians and maintenance workers of all kinds.
- A physically secure area is one in which unauthorized access cannot be gained by the use of ordinary tools and access would show obvious signs of damage. Some common items to check are:
  - Access doors should have their hinges inside the secure space.
  - Check for possible access through "drop" ceilings.
  - Mitigating measures typically consist of motion detectors connected to burglar alarms and/or video surveillance connected to a DVR.
- **If you are planning to use a mobile livescan unit**, and/or you are thinking of connecting your livescan wirelessly, or your livescan unit might possibly be stored in a non-secure location, please call DPS first so we can discuss the requirements with you before you purchase your livescan unit.

Nevada Specification Requirements

All livescans must be configured to the current Nevada Specifications prior to connection and be able to transmit SMTP. Your livescan must also have the ability to retrieve messages using a POP3 account. You and/or your vendor may obtain these specifications from one of the Livescan Coordinators listed on the Livescan Connection Cover Letter.

Site Security Inspection

Before DPS will allow your site to connect to the DPS network as well as indirectly via the MorphoTrust channeling gateway, the Information Security Officer (ISO) or the ISO's

designee may evaluate the security assessment in lieu of performing a physical site security inspection or as otherwise prescribed by the Division.

To be ready for an on- site security check by DPS staff:

- All physical security measures must be in place
- Your connection to SilverNet, DPS, or Internet service, as applicable, must be in place.
- All the network components for your local network up to and including the firewall that provides separation between Livescan devices and the general purpose network must be in place, including all configuration.
- The Livescan and/or printers do NOT need to installed or on-site for a security check for new installations.

Security Notes

- No wireless access may be installed inside the Livescan firewall.
- Any hard drive or non-volatile memory must be sanitized before the livescan can be stored in a non-secured location or transported by a person who is not authorized to access the livescan unit.
- The firewall should restrict outbound access to just the VPN tunnel, along with whatever is required to automate management of the livescan unit, whenever possible.

Turning Up Service

All activities, the administrative provisioning for livescan system settings, site security checks, establishing connectivity, and turning service on or off, are all initiated with a call to the DPS Fingerprint Examiner Unit. The primary contacts are Shanon Helget, (775) 684-6235, or Nicole Davis, (775) 684-6227. The Fingerprint Examiner Unit will coordinate all of the activities with all necessary stakeholders and will be a central point of contact for you.

All security issues discovered during the site security inspection must be addressed before submitting fingerprints electronically.

Compliance Auditing

Your site may be checked at any time to ensure compliance with current policies affecting livescan use, and we use the opportunity to provide education about any changes in policy. If any security issues are brought up during these visits, please act and respond promptly. This will keep you securely connected for fingerprint submission.

Thanks!